Israel: Information Operations Threats And Countermeasures

By Tomer Ben-Ari

***Editorial Abstract:** Mr. Ben-Ari calls for a more proactive response to cyber threats, in order to win on the new "cyber front." Proactive steps include controlling the number of terrorist websites and their content, creating a search and download detection engine for suspected terrorist activity, surveilling Internet communications devices, identifying insider help, and concluding international conventions and local legislation. Ben-Ari sees Israel's vulnerabilities as spam/phishing attacks and terrorist use of webcams. He also explores extremists perceptions of a hundred year war.*

Introduction

The use of information operations (IO) by terrorist organizations is here to stay. Conflicts with terror organizations such as Hizballah and Hamas show that with the use of IO, even attacking the civilian population can be achieved easily. As a result, Israel has changed its approach to IO within the last decade. The country's leadership realizes IO is a real threat that can easily create massive physical and cognitive damage, to civilians and military personnel alike. Several measures have been taken in order to protect critical infrastructure, to include countermeasures. Yet a defensive approach is not enough—we need a proactive approach in order to win a cyber war. The software solutions offered here focus on active counter-methods. Two vulnerabilities serve as immediate threats for Israel to confront: spam and phishing attacks; and the explosion of webcams as a concrete threat.

Israeli Defense Forces insignia. (Wikimedia)

IO Roadmap of Terror Organizations

Dr. Boaz Ganor, a well-known counterterrorism researcher, defines the potential of terror as the sum of the motivation and operational capability of terror groups. The use of IO directly increases both capabilities and motivation in a significant way, plus at a relatively low cost and minimal risk. The increasing use of IO warfare tools will surely increase the spread and magnitude of terror worldwide, as well as its sophistication and ability to avoid interception. The facts clearly indicate that the use of IO will become more popular in the years to come, due to Western societies' (followed by developing countries) increasing dependence on computer systems for all operations—in almost every aspect of life. Dr. Ganor claims that Al Qaeda's global terrorist warfare is one of the most dangerous threats ever mounted against mankind; furthermore, it is more lethal than the threat posed by the Cold War's nuclear confrontation between America and the Soviet Union. Dr. Ganor points out several characteristics of contemporary terrorism:

• The first characteristic is that Al Qaeda and its affiliates are not bound by any geographical or national restraints. Today al Qaeda and its affiliates are dispersed in many lands, especially in lawless regions, but also have cells in Western countries. The cyber world has no law, limits, or constraints. Computer systems and networks are interconnected and accessible from anywhere, thus there is no need to physically be present in some geographic area to exploit them. Additionally, there are many security flaws in current systems. It takes a long time to fix them, leaving them vulnerable for some time. Moreover, we don't know every vulnerability—there are lots of viruses and vulnerabilities found daily. As terrorists use the Web to organize, recruit, and gather intelligence (and exploit information) it will be much more difficult to fight terror groups, find them, or trace their operations. They are able to hide just about anywhere, do all communications over the Web, exploit vulnerabilities, and cause real damage.

• Second, Al Qaeda and its affiliates are interested in employing weapons of mass destruction represents a transition from conventional to non-conventional terrorism. There are cookbooks available on the Web offering "step by step" instructions on how to make bombs and other lethal weapons. By using Web communications it will be easier to interact with researchers that are trying to develop chemical, biological, and nuclear weapons, and are willing to sell their knowledge for extra income. It is relatively easy to influence people anywhere to develop these weapons, and to use them to serve mutual goals of both terror organizations and their collaborators.

• Third, Al Qaeda and its affiliates believe they are waging a "100 years" war, in which they will ultimately prevail, no matter how many years it will take to achieve their objectives. This is a non-rational perception of time. World leaders have a tough time convincing their civilian populations to fight such long wars, yet civilians demand immediate security. This perception of time by terrorists, the strength of terror movements, is opposite and irrational for nation states. Most believe current IO threats such as Distributed Denial of Service (DDOS) attacks, partial damage to government services, communication between service cells, and information gathering are still far less damaging than a 9/11 attack. Nevertheless, terrorist organizations believe that as the Web and computerized solutions develop in the forthcoming years, our lives will become captive to a handful of computers. This will enable them to find weak points in the civil and governmental systems,

and cause massive damage in the long run. Due to the fact that they only need to succeed a few times out of many attempts, it's only a question of time before they will be able to cause significant damage on an ongoing basis.

• Fourth, Al Qaeda's pre-9/11 organizational structure has changed from a structured, hierarchical organization with a decision making process based on command and control principles, into its current flat and cellular organizational structure. After losing much of its infrastructure in Afghanistan as well as the ability to move freely, Al Qaeda began using other Islamic terrorist organizations as proxies to carry out their operations. Spreading the message and recruiting over the Web can prove to be a tremendous unexpected proxy. By using simple cyber recruitment tactics, organizations like Al Qaeda's can easily outsource their operational attacks—even to individuals.

All of these factors indicate that information operations are here to stay. Countries must encourage research and the development of tools to resolve these and future IO threats, to avoid being surprised at the end of the day.

IO in Israel

Cyber threats have been in decision-maker and intelligence forces' crosshairs since computers started playing a major role in our defense forces and day-to-day lives. At first governments didn't see cyber threats as another war zone, but as a way of gathering critical intelligence information on forces, strategies, and facilities. In the past 10-12 years Israel has changed this thought process. Today Israel understands that cyber threats are actually another war front. Cyber attacks will not be directed only at defense forces, but will mainly attempt to interrupt and affect the civilian population. This occurred during the Second Lebanese War [2006], when Israel's adversaries attempted to demoralize the civilian population by aiming thousands of missiles at them. Through their massive exposure to computerized services, civilians will serve as a main front in a future cyber war. Damage to banking systems, traffic control systems, or major news websites (to include taking them hostage) can cause chaos, damage, and fear. In the past 10 years more and more government offices began providing Web services, making these more essential and more common in the public sector. Government and civil sector services are the main factors in our day-to-day lives. Continuing disruptions of critical infrastructure might raise the question "Can this government really defend and secure us?" Governments recognize that disruptions of websites, even if not causing an immediate security crisis, can motivate more and more people to try to hack and cause further problems.

Republic of Israel (Univ. of Texas)

Israel is facing increasing attacks on its computer infrastructure, averaging approximately 20-40 thousand attempted attacks every day, mainly against government websites and services. There is a real fear these may expand to more serious attacks: such as data corruption; data gathering and spying operations; traffic disruption; and the spread of disinformation thru media sites.

During the Second Lebanese War, Hizballah opened a website hosted in Iran. Launched in English, Arabic, and Farsi (and after the war in Hebrew), the site offered reports on the Israeli Defense Force (IDF) and the political situation in Israel. This Web effort was a well planned attempt to influence Israeli public opinion. It also turned out that Israel suffered from critical information leaks. Anyone could easily find movies, pictures, and operational charts that included frequency network channels, soldiers' equipment, and tactical memos. Classified information from the "Binat Jabel Fight" was also available. Binat Jabel is a village in southern Lebanon which is considered as Hizballah's main area. The Second Lebanese War saw intense fighting there, though the IDF eventually managed to take control of the town—a major turning point in that war. On the other hand, Hizballah had modern equipment on the battlefield including cameras. Photos and movies didn't find their way to the Web in an uncontrolled way. It is believed that rocket strike locations were reported to Hizballah in real-time via the Web, which helped them improve their aim. Further, a huge number of websites were defaced as protests against Israel, to include NASA, Microsoft, University of California at Berkeley, and US Government pages. The hackers used Structured Query Language (SQL) injection techniques to extract users' names and passwords, then used this access to change website content. In order to motivate supporters, especially the younger generation, Hizballah recently launched a computer game named "Special Forces 2." The game imitates events that actually happened, such as kidnapping soldiers, firing rockets on Israeli towns, and participating in guerrilla battles. Based on recent experiences, Israel changed its attitude toward the IO threat, and established units that will deal with this problem on a daily basis. These new organizations will provide preventive instructions, consulting options, and tools.

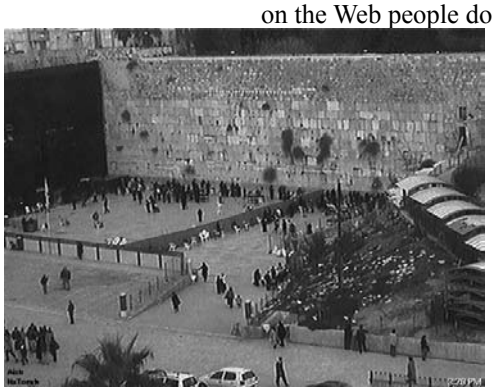
Defensive Operations

Israel's definition of IO is similar to Ivan Goldenberg's definition, who claims that information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy an adversary's information,

information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military, political, or business adversaries. This definition is sometimes minimized to the following: "Taking the offensive on the computer services of the enemy while defending one's own computerized services: defending and securing the secrecy of the service while maintaining its availability."

Israel has established the National Data Protection Authority (NPDA) to lead the way in information warfare measures. This authority is responsible for securing government offices and services from possible offensive operations. NPDA leads the research and countermeasures effort against any information warfare danger. The authority is under Israeli Shabak (Israel's internal security service, the equivalent of the US Federal Bureau of Investigation) supervision. In order to better deal with information warfare dangers, the prime minister's office has adapted a data protection doctrine to be applied to all government infrastructures defined as critical. Fundamentals of Israeli protection doctrine are:

• Information Mapping: Each office and critical institute would examine and categorize data as sensitive or non-sensitive information, according to two main parameters: classified information and vital information. The latter means information which needs to be kept available and reliable at all times. Each entity receives a risk analysis based on information exposure and use. This includes possible threats, current vulnerabilities, increasing risks, and countermeasures taken;



Western Wall webcam, Jerusalem. (Window on the Wall)

• The Human Factor: Offices must minimize human errors, theft, fraud, or misuse of information. Therefore, each employee should be questioned and checked thoroughly. Connections with outsourcing companies should be reduced to a minimum. Employee training is provided on how to identify and track a social engineering attack;

• Logic Protection: Each office will define a management policy for all the computer data systems. Each user will be able to access only the resources that were authorized to him. Password usage is a must. Biometric devices will be combined on some of the systems. Logical monitoring will look for suspicious acts within the system's log;

• Physical Protection: Employees must reduce the number of printed documents, limit access to printing rights, and prevent the exposure of classified information to optical or magnetic devices. Secure data transfer between different entities is required. Employees ensure only unclassified data is put on personal computers.

• Disaster Recovery Planning (DRP): Preventing disruptions and sabotage to an entity's ongoing work processes, and protecting critical processes from deliberate damage or unexpected failure are absolute necessities. This process will enable the quick restoration of the system to its former status before a collapse starts. Organizations must maintain status of their systems at all times.

• Network and Internet Security: Access to internal data should be limited based on management roles. There will be no direct connection between office data and websites. Office websites will have a secure zone for their computers. Establishing firewalls on all networks, plus consistently checking for Trojan horses, viruses, and other malicious software is required.

Countering Cyber Terror Methods and Recommendations

In order to win on the cyber front, we require proactive steps. In order to prevail in cyberspace, protection of valuable resources is not enough—we need offensive action in order to reduce a terrorist organization's impact.

• The first action to take is to control the number of terrorist websites and terrorist content on the Web. Here, one person can look like a whole army. It is very easy to appear to be a powerful and large organization by opening many websites, then generating content and traffic. Moreover, unlike real life, on the Web people do not die: their message can stay forever. A combination of DDOS attacks against terrorist websites, plus legislation that prohibits terrorist propaganda on the Web will significantly reduce the amount of terrorist content. We should also consider deliberate actions make some selected sites serve as "honey traps."

• The second action is to create a search and download detection engine. It is possible to know the IP address of the websites one visits, and the files downloaded. If searched information looks suspicious, for example too many searches for maps, plans, and data of the Empire State Building, then security authorities should check out the person(s) making those queries

• Third is surveillance of Internet communication devices. Emails describing the planned 9/11 attacks were found on Al Qaeda computers. These communications are not limited to email, but extend to other text and voice communication devices such as Skype or MSN Messenger. Detection software searching for suspicious information transfers can detect extremist actions prior to implementation.

• Fourth, one must identify insider help. An employee of a critical organization can help extremists get control of computer systems within an organization. Possible scenarios are opening specific ports or connecting a wireless device to the network. With insider help, extremists can remotely log into the network, access software, and cause damage. A system to gather and analyze all system transactions in an organization can recognize abnormal behavior, which may imply a potential attack.

• The fifth action, probably the basic factor for all of the above counter-solutions, is legislation. Currently there are no

strict rules on what is legal or illegal in the cyber arena, thus many loopholes exist. In order to win the battle against cyber terror, we should be prepared to pay a price in personal freedom. What rights are we willing to give up when using the Web in order to ensure security? This question is critical and we should answer. Further, existing rules vary from one country to another. In order to succeed in this war, we must legislate strict rules—and international conventions must be signed.

Immediate Cyber Threats

Many of the terrorist threats that are being discussed today require intensive and sophisticated development. Yet two types of threats can be developed quickly, using off-the-shelf technologies and a relatively small group of people. These immediate concerns are spam/phishing attacks, and webcam exploitation.

• Spam and Phishing can become attractive to terrorist groups, not merely as a tool to spread their messages, but also to raise funds and recruit members. More importantly, spam can be used by terrorists to influence non-members of a terrorist group to carry out attacks that coincide with the terrorists' goals and plans. Such connections allow coordinate among a dispersed, heterogeneously motivated network of activists. Now we commonly assume that some Islamic terrorist organizations will only recruit staunch believers to carry out attacks (especially suicide attacks), but in the future they may use "outsourcing" techniques—and will find the right justification for doing so. The trigger may be lack of resources, or the clear logistical and operational benefits of "outsourced" activities. Worse, it may result in higher quality attacks.

The main features that make spam and phishing attractive to terrorists are:

1. Anonymity and difficulty of tracing;
2. Low cost to reach a large audience, hence the ability to engage in a large number of initiatives;
3. Leverage in reaching new and otherwise inaccessible audiences;
4. Ability to recruit operatives from within the society under attack;
5. Ability to spread fear, even without any action being taken.

After detecting and communicating with possible carriers, their communications can be moved to more secure systems.

•Webcams for Surveillance and Information Gathering: These days there are many cameras on the Web. These are very simple and cheap to install; some are wireless and others satellite-based, and all are reasonably priced. Some webcams are private, showing entertainment places, malls, and private homes, while others are government-based, showing tourist places, traffic junctions, and streets. Webcam host sites can also serve as a webcam search engine. Combined with software products such as *Google Maps* and *Microsoft Live Maps* that use cameras combined with static photos, we can view every street corner. In the future, as network pipes become wider and network traffic faster, we will have live scenes on those same street corners.By exploiting these webcams, terror organizations can acquire intelligence on specific targets without stepping foot on them. Moreover, video information can be analyzed by computer vision algorithms. Based on technology available today, it's not difficult to access a specific webcam and analyze its data stream. For instance, how many people cross a specific street each day and at what times, or how many police cars pass? Such software would create reliable, long-term, well-analyzed information about happenings in many different places. Extremists could separately and easily monitor multiple locations, without putting their spies at risk.

Conclusion

Israel believes that IO will become an essential weapon in the future in any war or actions against terrorists. Since it will become easier to hit Western society using IO methods, Israel must be prepared to take offensive methods and measures. Resources should be invested in finding vulnerabilities and fixing them. Catching terror groups before their actual mission and detecting IO attacks prior to the point where massive damage is done is the goal of offensive actions. Legislation and worldwide cooperation should be enhanced as well in order to generate effective solutions.